Report of Review Committee on Open APIs: Promoting Open Innovation

July 13, 2017

Review Committee on Open APIs

Secretariat: Japanese Bankers Association (JBA)

Foreword[1]

In recent years, "open APIs," which disclose methods for connecting with banking systems to other companies, have attracted increasing attention as a tool for enhancing financial services through collaboration with financial institutions and Fintech companies, etc. In the Japanese banking industry, many banks have now begun considering the possibility of utilizing open APIs.[2]

An API (Application Programming Interface) generally refers to connection specifications that enable functions and managed data of an application to be accessed and used by another application. APIs that allow access by other companies and such (hereafter referred to collectively as "third parties" or individually as a "third party") are known as "open APIs."

Open APIs in the financial sector are currently in the trial-and-error phase in various countries around the world. While there are many issues which need to be organized, the collaborative innovation enabled by open APIs is highly compatible with Japan's business culture, and our banking industry can become a world leader in this area.

In the report of the Working Group on Payment and Transaction Banking (announced December 22, 2015) and the Japanese Government's "Japan Revitalization Strategy 2016: For the Fourth Industrial Revolution" (cabinet decision as of June 2, 2016), policies for the collaboration of the banking industry with financial administration authorities considering the opening up of banking system APIs (interfaces) have been formulated to enable the creation of various financial services in partnership with banks while also ensuring information security.

In light of this, JBA established the Review Committee on Open APIs, whose members include companies in the banking sector, IT companies, Fintech companies, academic experts, lawyers, consumer associations, and relevant government authorities, to deliberate the adoption of open APIs in the banking sector ("banking APIs").

In order to prepare this report, the Committee solicited opinions from various perspectives, including those of customers, Fintech companies and financial institutions, through the participation of a wide range of related-parties. With the aim of stimulating open innovation in Japan in an impartial manner, the report seeks to present information that balances the promotion of innovation with user protection.

Based on the Committee's deliberations, this report summarizes public-private initiatives intended to promote the use of open APIs in order to enhance financial services and improve bank user convenience in Japan through win-win-win relationships between customers, Fintech companies, and financial institutions.[3]

---

[1] This is a provisional English translation of the original Japanese document and is provided for reference purposes only.

[2] According to the survey conducted by JBA in June 2016, 48% of Japanese banks were in the process of considering the use of open APIs.

[3] The Committee hopes that this report will also serve as a reference for non-banking companies who wish to engage in open APIs.

Table of Contents

Members of Review Committee on Open APIs (as of March 2017)

Members	Shoji Masuda	Executive Officer and General Manager, IT Planning Department,, Sumitomo Mitsui Banking Corporation
	Hiroki Kameda	Executive Officer & Group Head, Information Systems Group & General Manager, System Planning Division, The Bank of Tokyo-Mitsubishi UFJ, Ltd.
	Masahiko Kato	Specialist Officer, IT & Systems Group, Mizuho Financial Group
	Hiromitsu Umehara	Director/General Manager, Corporate Planning Department, Shizuoka Bank
	Susumu Sasaki	General Manager, Channel Development Division, Fintech Promotion Office, North Pacific Bank, Ltd.
	Norifumi Yoshimoto	General Manager, Fintech Business Planning Dept., SBI Sumishin Net Bank, Ltd.
	Daisuke Sahata	Executive Manager, e-Business Sales & Planning Section, NTT Data Corporation
	Shigeo Hagawa	Manager, Financial Industry Solution No.1, BK/FM Service, Global Business Service, IBM Japan, Ltd.
	Hiroki Maruyama	Representative Director, Fintech Association of Japan, and Representative Director, Infcurion Group
	Mark Makdad	Director, Fintech Association of Japan, and Sales Head, Moneytree
	Toshio Taki	Director, Money Forward, Ltd., and Fintech Institute/FINOVATORS
	Masakazu Masujima	Partner, Mori Hamada & Matsumoto
	Tetsuo Morishita	Professor of Law, Sophia University Law School
	Atsushi Koide	Professor, Faculty of Law, Gakushuin University
	Motonobu Matsuo	Deputy Director-General, Planning and Coordination Bureau, Financial Services Agency
	Jutaro Kobayashi	Director General, Planning Department, The Center for Financial Industry Information Systems
	Yumiko Nagasawa	Executive Director, Foster Forum
Observers	Naoyuki Iwashita	Deputy Director-General, Payment and Settlement Systems Department/Head of FinTech Center, Bank of Japan
	Sawaichiro Kamata	Senior Advisor, Policy Making Headquarters, Japan Securities Dealers Association
	Seiji Nakano	General Manager, Payment Solution Development Department, UC CARD Co., Ltd./Japan Credit Card Association
Secretariat	Japanese Bankers Association	

Outline of Committee Meetings

The Committee has held briefing sessions with the secretariat and heard opinions from related-parties and experts. The Outline of each meeting's activity is provided below. In addition, an overview of the agenda at each session is available in the summaries of proceedings published on the website of JBA.

First Committee Meeting: November 2, 2016

- Briefing session, "Overview of the Committee's Establishment and Discussion Point Memos"
- Briefing session, "JBA Survey Results"
- Briefing session, "Overview of the U.K.'s Open Banking Standard"
- Fintech Association of Japan, "Japanese Fintech Companies and Financial Institutions Create New Markets through Open APIs and Collaboration"

Second Committee Meeting: December 5, 2016

- Briefing session, "Outline of Discussion Points Relating to Security Principles and User Protection Principles (Proposal)"
- Fintech Association of Japan, "Consideration of Risks When Using Read/Write APIs"
- The Center for Financial Industry Information Systems (FISC), "Expert Review Committees Relating to Fintech at Financial Institutions"
- NTT Data, "Introducing Security-Related Rules of PSD2"

Third Committee Meeting: December 8, 2016

- Briefing session, "Security Measures for Open APIs and Basic Approach to User Protection (Preliminary Discussion)"
- Keisuke Nakamura, Center for Information Technology Studies, Institute for Monetary and Economic Studies, Bank of Japan, "TPPs and Open APIs in the Financial Sector: Key Security-Related Issues"

Fourth Committee Meeting: December 16, 2016

- Briefing session, "Security Measures for Open APIs and Basic Approach to User Protection (Revised Proposal)"
- Briefing session, "Revisions Based on Comments in Previous Session and Approach"

Fifth Committee Meeting: December 21, 2016

- Briefing session, “Security Measures for Open APIs and Basic Approach to User Protection (Proposal)”
- Infcurion Group, “Comments on Security Measures for Open APIs and Basic Approach to User Protection (Proposal)”
- Moneytree, “Comments on Security Measures for Open APIs and Basic Approach to User Protection (Proposal)”
- Money Forward, “Comments on Security Measures for Open APIs and Basic Approach to User Protection (Proposal)”
- Freee, “Comments on Security Measures for Open APIs and Basic Approach to User Protection (Proposal)”
- Zaim, “Comments on Measures for Open APIs and Basic Approach to User Protection (Proposal)”
- W3C, “W3C Web API Standardization Trends”

Sixth Committee Meeting: February 2, 2017

- NTT Data, “Introduction of Open API Initiatives for ANSER”
- IBM Japan, “Approach to Banking API Standards”
- Hitachi, “Reference Documents for Considerations Relating to Open API Standardization”
- Fintech Association of Japan, “Fintech Companies’ Requests with Regard to Banks’ Open API Specifications”

Seventh Committee Meeting: February 8, 2017

- Briefing session, “Discussion Document: Standardization of API Specifications (Draft)”
- OpenID Foundation, “Financial Grade OAuth & OpenID Connect”

Eighth Committee Meeting: February 20, 2017

- Briefing session, “Report of Review Committee on Open APIs (Intermediate Version) (Draft)”
- IBM Japan, “Examples of API Use by Governments in Other Countries and Status of Deliberations”

Ninth Committee Meeting: February 27, 2017

- Briefing session, “Report of Review Committee on Open APIs (Intermediate Version) (Draft)”

- Financials ISAC Japan, “About the Fintech Security Working Group of Financials ISAC Japan”

Tenth Committee Meeting: June 28, 2017

- Briefing session, “Report of Review Committee on Open APIs (Draft)”
- Briefing session, “Standardization of Electronic Message Specifications for Open APIs in the Banking Sector”
- FISC, “FISC Initiatives Relating to Fintech”

The Committee would like to express its sincere gratitude to everyone involved who provided valuable suggestions and took part in the presentations at each meeting.

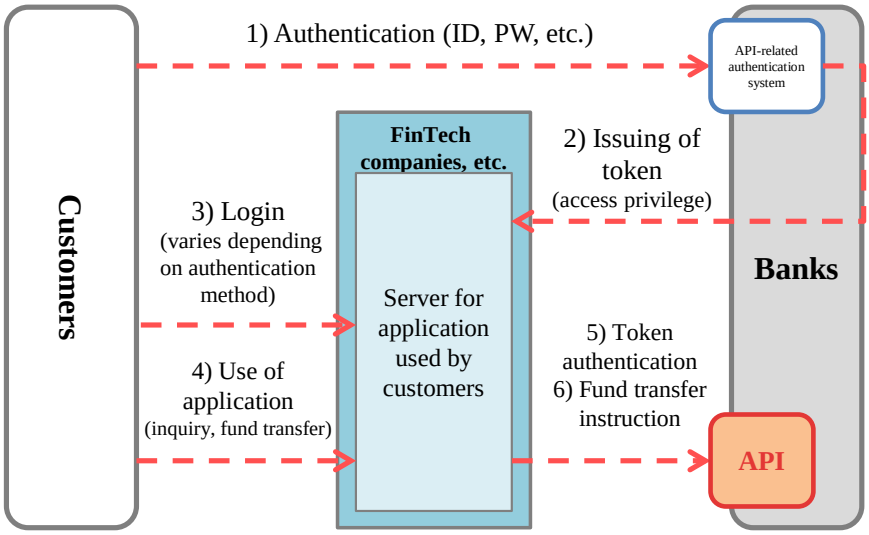
1. Introduction

1.1 Purpose of Report

- With developments in IT expected to significantly alter the nature of financial business, open innovation should be considered as one of the basic strategies adopted by financial institutions going forward.

- Open API technology makes it possible to securely share data with other companies[4] on open networks. However, its significance goes beyond mere data sharing: it is a key technology that enables financial institutions and other companies to combine their information and services and to pursue open innovation through mutual efforts to develop new ideas.

Figure 1: Basic Framework of Open APIs (OAuth 2.0)



*1: The is an extremely simplified representation of the communication/workflow that is actually implemented
*2: Typically, data communication is handled via an Internet connection.

- Public-private partnerships are under way in various other countries, such as consideration of API specification standardization (e.g., the U.K.'s Open Banking Standard), addressing issues related to promoting the use of APIs, and developing laws to promote open APIs while ensuring user protection.

- In light of these circumstances, the Committee has deliberated how open APIs in the banking sector (banking APIs) should be implemented as a public-private initiative aimed at promoting the use of open APIs in order to enhance financial services and improve bank user convenience in Japan.

[4] Other parties who could collaborate with banks via open APIs include businesses in industries such as distribution/retail and service as well as Fintech companies (hereafter referred to as "Fintech companies, etc.").

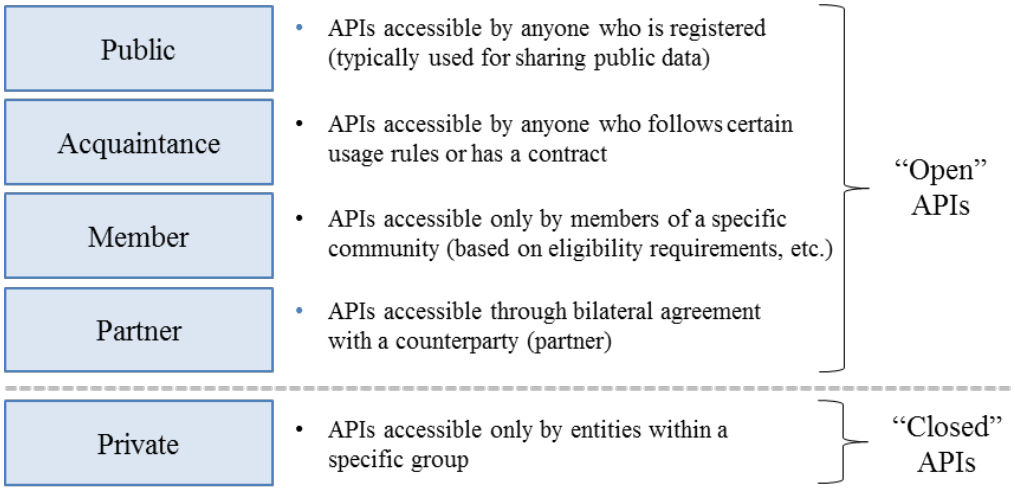
- This report is intended to provide the norm for the implementation of open APIs, based on discussions involving the Committee members, who represent a wide range of related-parties, including the banking sector, IT companies, Fintech companies, academic experts, lawyers, consumer associations, and relevant government authorities. The Committee hopes that this report will be of considerable value to parties engaged in open APIs.

1.2 Applicable Scope of Proposals

- This report covers open APIs in the banking sector (banking APIs). However, this does not preclude its use as a reference for open API-related initiatives in other fields. In addition, this report has been written based on the assumption that API-based third parties will not be bank agents or outsourcing contractors of banks.[5]

- In general, it is assumed that openness of bank open APIs will fall into one of the four categories below. The proposals in this report apply for all four categories.

Figure 2: Openness Categories for Open APIs



Source: Prepared based on Euro Banking Association, "Understanding the Business Relevance of Open APIs and Open Banking for Banks," May 2016

[5] This does not preclude the report being used as a reference if the companies involved in an open API are bank agents or outsourcing contractors of banks, but in that case, it should be noted that various user protection regulations based on the Banking Act shall be applied and take precedence over the report's proposals.

2. Standardization of API Specifications

2.1 Basic Approach

a API specification is a key consideration from the perspective of both: 1) maintaining security standards and ensuring user protection; and 2) promoting open innovation through collaboration and partnerships between financial institutions and Fintech companies, etc.

- Normally, API specifications are stipulated upon mutual discussion between banks and Fintech companies, etc., with the aim of facilitating collaboration using APIs. The versatility and scalability of the specifications are basically designed based on each bank's strategy. When deciding on specifications, there are many cases where the parties involved select one of multiple options that are technologically equivalent, and if there are no standards and norms, it is possible that specifications will vary considerably between banks.

- With a view to simplifying N-to-N connections between banks and Fintech companies, etc., and promoting open innovation, it is preferable to stipulate certain standards and norms for specifications and develop environments that enable connections based on common specifications as much as possible.[6] Stipulating specification standards and guidelines will also help to reduce system development costs of banks and the costs of communication between banks and Fintech companies, etc.

- It is also necessary to stipulate basic specifications that APIs need to meet in order to maintain security standards and ensure user protection.

b At the same time, while considering standardized API specifications that will address the above problems, it is also necessary to bear in mind the following points:

- If the programs that comprise APIs are standardized across financial institutions, it has been noted that any vulnerabilities discovered in these programs could have an impact on a large number of financial institutions.[7]

- If it is decided to stipulate comprehensive, detailed standards of an API specification, it is possible that API development by related parties will be halted until the standards have been finalized; moreover, API specifications of Japanese banks will converge with these standards, which means that the scope of Fintech services which can be implemented in Japan will be restricted, and there is a risk that rather than enabling and facilitating open innovation, standardized specifications will impede it.

---

[6] In the survey conducted by JBA in June and July 2016 (effective response rate: 99 out of 120 full member banks), many member banks made requests for standardization of specifications and development of common standards.

[7] See Keisuke Nakamura (2016), Center for Information Technology Studies, Institute for Monetary and Economic Studies, Bank of Japan, "TPPs and Open APIs in the Financial Sector: Key Security-Related Issues" (p. 11). Nakamura's report states that "standardization should be restricted to data description languages, architecture styles, function names and return values, and it is preferable for individual programs to be created and managed independently by each financial institution."

- While there are movements toward standardization of API specifications in various countries,[8] concrete specifications have not been decided, and it is difficult to be sure of the form that standard API specifications aimed at facilitating connections between Japanese banks and overseas Fintech companies, etc., will take.

c In light of these points, the Committee has prepared three sets of guidelines for parties currently involved in API development ("Guidelines"): 1) "Development Principles" (Section 2.2) to be kept in mind by those developing APIs, 2) "Development Standards" (Section 2.3) which recommend concrete API specifications, and 3) "Electronic Message Specification Standards" (Section 2.4) which stipulate standard items and definition guidelines for electronic messages.[9]

d In preparing these Guidelines, a conscious effort has been made to define purpose and context so as to avoid impeding innovation and the development of cutting-edge initiatives by stakeholders (see the start of each section) and to allow stakeholders as much flexibility as possible in customizing individual APIs, adapting to technological advances, and applying new technologies based on their own judgment.

e The Guidelines are not intended to prevent individual banks and Fintech companies, etc., interested in collaborating on APIs from considering specifications upon separate discussion or impede efforts to ensure the versatility and scalability of specifications based on individual bank open API-related strategies; on the contrary, they are designed to actively encourage such efforts.

f During the discussions relating to this report, Fintech companies expressed many expectations for the detailed API specifications to be developed by banks. Since many of these expectations may be useful as references for individual banks when considering API specifications, they have been indicated at the end of this chapter in Section 2.5 ("Other") for reference. When making revisions to the Guidelines in future, the Committee will continue to bear these expectations and requests in mind as needed.

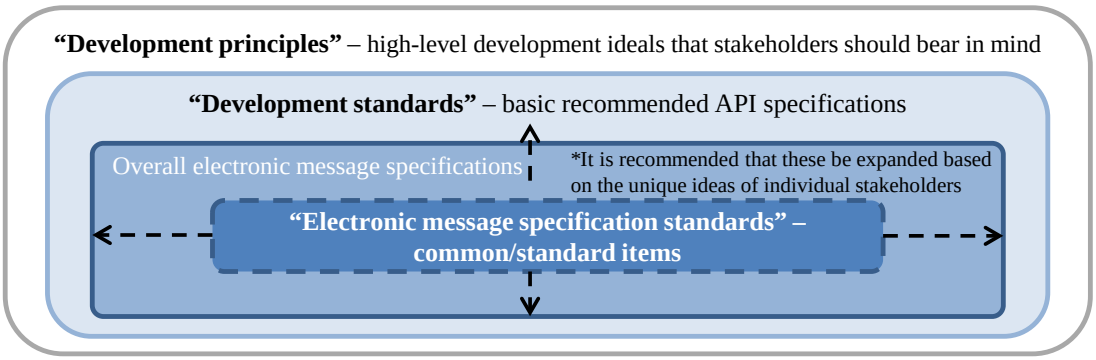
g The Committee hopes that this report will serve as a reference for guidelines for those engaged in developing APIs[10] and help to stimulate open innovation in Japan.

[8] For example, the U.K.'s Open Banking Standard (2016) sets forth principles for standardizing API specifications (7a. 4 API Standards) and the definition and scope of data (7a. 8 Data Standards), but at the present time, standards for architecture styles, data representation formats, and so forth have only been outlined in broad terms.

[9] See "3. Security Measures and User Protection" with regard to specifications for provision of access privileges, authentication methods for individual transactions, management of access privileges/tokens, validity periods for tokens, communication methods and handling incidents of unauthorized access.

[10] It is expected that these guidelines will also serve as a reference for businesses other than banks engaged in open APIs.

Figure 3: Relationship Between Development Principles, Development Standards, and Electronic Message Specification Standards



2.2 Development Principles

2.2.1 Purpose and Context of Development Principles

a These development principles stipulate a high-level development ideal that those involved should bear in mind when developing and deciding on specifications for APIs.

b Open APIs are a key technology for enabling open innovation, and it is expected that this technology will be used to deliver a wide range of business models and services in the future. It would be difficult and inappropriate to stipulate standard specifications that cover all of these, including innovative financial services studied through partnership and collaboration between individual banks and Fintech companies, etc., and it is not the intention of this report.

c On the other hand, open APIs provide other businesses with access to banking system connection specifications and are fundamentally different from banking systems used exclusively by banks. Therefore, regardless of the type of API, open design concepts intended for use by other companies are required.

d Based on this perspective, the purpose of these development principles is to indicate development-related ideals that those involved should bear in mind when developing and deciding on specifications for APIs and support the establishment of an environment that fosters open innovation.

e The development principles include principles that are already being put into practice by those involved in developing APIs, and whenever possible, examples of beneficial initiatives are presented as reference for those who wish to develop new APIs. The information is as of June 2017.

2.2.2 Development Principles

Principle 1: Make designs and explanations simple and easy to understand from the perspective of API users

a Because APIs will be used by other companies, designs and descriptions should be made simple and easy to understand for the benefit of API users.[11] Such designs and

[11] It is preferable to avoid needlessly complicated, distinctive specifications. Generally speaking,

descriptions will also help to limit the risk of bugs occurring on the API user side, facilitate handling differences in specifications between banks for Fintech services that connect to multiple banks, and ensure the versatility and scalability of APIs developed through collaboration between banks and other businesses.

b When creating designs and descriptions, it is preferable to closely consult and collaborate with businesses that have the potential to connect through API.[12] Moreover, once API specifications have been decided, for those areas of the specifications that involve other parties, it is recommended that misunderstandings and misperceptions be prevented by preparing straightforward instructions (specification sheets) which do not make use of specialized in-house banking terms, financial sector acronyms and such.

c Creating simple designs and descriptions means, for example, identifying the items required for actual services and then providing specifications for them; it does not mean integrating or merging multiple items of different types and natures solely for the purpose of reducing the number of items in messages. In general, system design will be simpler and more versatile for other parties if they handle the integration of separate items, rather than having to separate already integrated items before incorporating them into their system.[13]

d The following are some examples of initiatives by leaders in the development of open APIs with regard to creating simple, easy-to-understand designs and descriptions with API users in mind:[14]

- Specifying names for URIs that enable API functions to be identified. URIs are described so that they have a high level of readability and are easy to modify.
- Making URI description rules consistent within each bank and using commonly used (easily understood) nouns in descriptions.
- Creating specifications that enable data to be designated by other connected parties (while avoiding specifications that affect any information other than the designated data).
- Creating specifications that provide detailed information so that other parties can identify the causes of errors.

Principle 2: Ensure appropriate security level for the relevant API type

a Since banking APIs involve the provision of highly confidential information belonging to banks, it is necessary to ensure that the security level should be appropriate for respective types of API functions. See Chapter 3 (“Security Measures and User Protection”) with regard to specific security measures and standards, including authentication and communication methods.

b In ensuring the security level, it is necessary to set an appropriate level of granularity

---

user-friendly APIs are those whose specifications can be understood and used by users even if they do not understand the specifications of the underlying banking systems.

[12] However, this does not mean they should reflect other party requests in a one-sided manner.

[13] During the Committee’s discussions, the Fintech Association of Japan, a member of the Committee, expressed the following opinion: “When it comes to the granularity of electronic messages, the more detailed they are, the better.”

[14] These include examples of initiatives related to APIs currently being developed. The same applies throughout this chapter.

for the scope (functionality) of each API that is provided and to make sure that third parties cannot use APIs whose security level exceeds the authority granted to them.[15]

c Since the techniques employed in cyberattacks and other cybercrimes are becoming more and more sophisticated each year, it is necessary to pursue ongoing improvement, review, and enhancement of API security measures and standards in collaboration with other involved parties.[16]

d If API specifications are made available to the general public, it is necessary to consider what impact this could have on security.

e The following are some examples of initiatives by leaders engaged in the development of open APIs with regard to ensuring API security standards:

- Encrypting and protecting communication pathways between banks and other parties using TLS, in accordance with BCP 195.
- In addition to typical security measures such as XSS and XSRF, implementing adequate countermeasures for API-specific vulnerabilities, such as JSON hijacking.[17]
- Limiting the number of API calls and implementing measures for handling errors that occur if a request exceeds the limit value.
- Implementing a function to revoke (invalidate) tokens, assuming unintended API operations will be performed by users.
- Introducing identifiers in order to distinguish specific transactions, such as transaction numbers or ID numbers for connected parties.

Principle 3: Ensure compliance with de facto standards, API standards in other countries, and international standards

a In cases where international standards exist and are available for reference, it is recommended that they be used whenever possible. For example, it is standard to use RFC3339 or ISO8601/JISX0301 as the representation format for dates and times and ISO4217 as the representation format for currency codes. In addition, as of June 2017, UTF-8 has effectively become the de facto standard for character encoding.

b Recommended basic specification for architecture styles, data representation formats and authorization protocols are stipulated in Section 2.3 (“Development Standards”) with the aim of ensuring compliance with de facto standards, API standards in other countries, and international standards.

c The following are some examples of initiatives, intended to ensure compliance with de facto standards, by leaders engaged in the development of open APIs:

- Specifications are designed with compliance in mind, after surveying API specifications at other banks, including those in other countries.
- Efforts are made to use standardized HTTP specifications, including status codes, whenever possible, and to minimize the use of proprietary specifications.

---

[15] See “Management of access privileges/tokens” in Chapter 3 (“Security Measures and User Protection”).

[16] Also see Section 3.3.5 (“Continuous Improvement, Review, and Enhancement of Security Measures”).

[17] This refers to theft of information sent from an API using JSON by a third party with malicious intentions.

Principle 4: Control the impact of specification changes on API users

a Since changes in API specifications will also have an impact on third parties (API users), such as requiring program changes, it is necessary to take appropriate steps to control the impact of such changes. There is a possibility that banking APIs will perform some of the functions of financial/settlement systems, so if a service provider suddenly becomes unable to access an API due to specification changes, there is a risk this could disrupt or otherwise impact many users (depositors) of the third party's services.

b In order to limit the impact of specification changes on third parties, APIs should be designed in advance to provide as much versatility and scalability as possible, and it is preferable to be designed considering the possibility of specification changes (addition or termination of functions, bug correction, data format modification and such). These measures will also help to reduce API specification modification costs at each bank.

c In order to prevent unilateral specification changes disrupting third parties, as a rule it is necessary to provide sufficient advance notice when changes will be made. Furthermore, it is recommended to run both the new and old versions in parallel for a certain period even after switching to a new version or to release new versions that include the old specifications.

d In the case of Partner open APIs, it is usually possible for banks to identify the third party, which makes it relatively easy to provide advance notification of changes. However, in cases involving provision of public information via a public open API, there are cases where banks will not be able to identify the providers accessing the API. Furthermore, even in the case of partner open APIs, if third parties are allowed to access the API without notifying the bank,[18] there are cases where the bank may not fully understand the impact of specification changes. Therefore, before proceeding with any specification changes, banks should take care to properly determine the extent of their impact.

e Specific recommended version management methods are stipulated in Section 2.3 ("Development Standards").

f The following are some examples of initiatives by leaders engaged in the development of open APIs in order to control the impact of specification changes on API users:

- Creating a development portal and establishing an environment where third parties can conduct tests before releasing new versions.
- Even when specifications are changed, APIs are designed in advance to ensure backward compatibility as much as possible.

2.3 Development Standards

2.3.1 Purpose and Context of Development Standards

a These development standards provide recommendations for basic API specifications, particularly with regard to the following four areas: 1) architecture style, 2) data

[18] See "Handling third parties of the third party" in Chapter 3 ("Security Measures and User Protection").

representation format, 3) authorization protocol, and 4) version management.

b The development standards are intended as guidelines to be used by those involved in API development when selecting basic specifications, with the aim to reduce the social costs arising from an excess of multiple specifications and to support the creation of an environment that fosters open innovation.

c It is up to individual banks to consider and decide whether to comply with these development standards.[19] It is essential to select appropriate, highly compatible specifications based on discussions with third parties, the nature of provided services, and other factors.[20]

d The basic specifications recommended in these development standards are designed to comply with specifications supported by API users (including those in other countries) and standards in effect in other countries (e.g., the U.K.'s Open Banking Standard) as of June 2017, based on the development principles outlined in Section 2.2.

e The Committee is aware that these development standards risk becoming obsolescent with the advent of further technological innovations. They will therefore be revised as needed in light of technological advances. Under the administration by JBA, modifications will be made while taking into account the views of various related-parties, such as banks, IT companies and Fintech companies, etc.

f The development standards are not intended to prevent individual banks from using cutting-edge specifications or technologies other than those recommended here. When it comes to security-related specifications in particular, if there are more recent specifications that can help ensure more robust security standards, it is recommended that those specifications be adopted.

2.3.2 Development Standards (as of June 2017)

a In terms of architecture styles, the use of REST[21] is recommended, while HTTPs is recommended for communication protocols. For REST, it is recommended that the design conform to the Richardson Maturity Model[22] Level 2 (introduction of HTTP verbs such as GET, POST, PUT, DELETE, etc.).[23] As of June 2017, these are the most

---

[19] These development standards are simply standards, not regulations. Some banks which have already developed APIs can take various initiatives aimed at complying with these standards when upgrading versions or introducing replacements.

[20] These development standards are aiming to support the creation of an environment that fosters open innovation based on N-to-N connections. In the case where APIs presuppose 1-to-1 (individual-type) connections or 1-to-N (infrastructure-type) connections, consideration may also be given to the use of different specifications according to the nature of the tasks or the details of the service. For example, XML format is established as a technical standard. Furthermore, as of June 2017, the W3C (World Wide Web Consortium; a non-profit organization that promotes the standardization of various technologies used online) is considering a system (payment request APIs) that uses user browsers to send settlement instructions directly to banks.

[21] REST stands for Representational State Transfer. It is a design principle for linking software and data.

[22] Refer to https://martinfowler.com/articles/richardsonMaturityModel.html.

[23] The Richardson Maturity Model also stipulates a Level 3 design level (HATEOAS: hypermedia as the engine of application state), but as of June 2017, its use is not necessarily widespread, so it has not

common specifications for APIs.

b In terms of data representation formats, JSON[24] is recommended. With REST, it is possible to use a variety of data representation formats, including JSON and XML. Since JSON enables simple, lightweight description of structured data, it is the most common format for newly developed APIs as of June 2017.

c With regard to authorization protocols, the OAuth 2.0 authorization framework[25] is recommended. With regard to detailed specifications for applying OAuth 2.0 to APIs in the financial field, standardization efforts are currently being undertaken by the OpenID Foundation Financial API Working Group (FAPI WG) as of June 2017, with a view to ensuring security standards. It is desirable for banks to comply (or give consideration to comply) with the specifications when this organization implements detailed specification for applying OAuth 2.0.[26]

d With regard to version management, Semantic Versioning[27] is recommended. With a view to controlling the impact of specification changes on API users, specification change levels are managed using categories such as major changes, minor changes and patches.

2.4 Electronic Message Specification Standards

2.4.1 Purpose and Context of Electronic Message Specification Standards

a The aim of electronic message specification standards is to provide guidelines for standard API message-related items and definitions[28]

b The approach to electronic message specification standards may be selected from the following options:

i. Stipulating complete, detailed electronic message specification standards that function if implemented as is, including the structure, items, values and parameters of electronic messages (e.g., JBA IC cash card standard specifications[29])

ii. Stipulating only standard items and definitions for API messages, based on the assumption that other specifications will be stipulated and developed as needed through discussion between banks and Fintech companies, etc., interested in working together on APIs (e.g., the U.K.'s Open Banking Standard [30])

---

been adopted as the design level in these development principles.

[24] JSON stands for JavaScript Object Notation. It is a lightweight data description language designated in RFC7159.

[25] Refer to https://oauth.net/.

[26] In cases of non-compliance, this includes consideration of reasonableness and tolerance.

[27] Refer to http://semver.org/.

[28] With regard to detailed specifications for OAuth 2.0, since standardization efforts are currently being undertaken by the OpenID Foundation Financial API Working Group (FAPI WG) as of June 2017, this chapter stipulates only electronic message specifications for API-related services.

[29] For security reasons, JBA's IC cash card standard specifications stipulate usage agreements and propose that specification sheets be restricted to parties who have been approved by JBA.

[30] With regard to the standardization of specifications, the U.K.'s Open Banking Standard (2016), with a view to balance innovation and stability, adopts an approach that stipulates "core" standards (areas that are not easily changed) to be used as a common resource in all business fields while enabling related-parties to freely diverge from or expand on other specifications (see Section 7a.2.1). However,

iii. Not standardizing electronic message specifications and relying on the establishment of de facto standards (e.g., this corresponds to specifications for web APIs released by general businesses and Fintech companies, etc.)

c While each of the above options has its pros and cons, the Committee has decided to pursue standardization based on method ii for the time being, in light of the social costs; 1) the cost involved with stipulating complete, detailed electronic message specification standards (e.g., costs of formulating, maintaining, and revising the standards; cost of impeding innovation) and 2) the cost relying on the establishment of de facto standards (e.g., costs of variation between specifications until such standards are established; costs associated with difficulties in processing and aggregation/integration for Fintech services due to distribution of data without consistent definitions; costs incurred due to misunderstanding by users).[31]

d The purpose of electronic message specification standards is to ensure the consistency of definitions for basic items and data used in Fintech services, simplify processing and aggregation/integration for third parties, and prevent misunderstanding by users, thereby supporting the creation of an environment that fosters open innovation.

e As with the development standards in Section 2.3, it is up to individual banks to consider and decide whether to comply with electronic message specification standards.[32] Furthermore, it is important that final specifications do not simply comply with the standards in a rigid manner but instead are decided by taking into consideration the versatility and scalability of APIs, discussions with third parties and the nature of services.

f The Committee is aware of the risk that electronic message specification standards may become obsolete with the advent of future technological innovations and such. They will therefore be revised as needed in light of technological advances and other trends. Under the administration by JBA, modifications will be made while taking into account the views of various related-parties, such as banks, IT companies, Fintech companies, etc.

2.4.2 About Electronic Message Specification Standards

a Electronic message specification standards will be formulated under the administration by JBA while taking into account the views of various related-parties, such as banks, IT companies and Fintech companies, etc.

b In formulating electronic message specification standards, the Committee asks related-parties to bear in mind the following points:

- In terms of the scope of application when formulating electronic message

---

as of June 2017, these core standards had not yet been finalized or published.

[31] In Japan, given that there are many cases of systems developed by a specific IT company being jointly used by multiple banks, especially regional financial institutions, and standardization of specifications for each common system is being undertaken through the efforts of individual IT companies, the Committee deems it unlikely that excessive differentiation of specifications will occur even if complete, detailed electronic message specification standards are not stipulated.

[32] These electronic message specification standards are simply standards, not regulations. Some banks which have already developed APIs can take various initiatives aimed at complying with these standards when upgrading versions and introducing replacements.

specification standards, they should be predicated on APIs that connect multiple banks and Fintech companies, etc. (i.e., they will be shared by banks), and for the time being, they should cover the following deposit-related activities: 1) account balance inquiries, 2) account activity inquiries, and 3) transfers.[33]

- With regard to account balance and account activity inquiries in particular, as of June 2017, some Fintech companies, etc., would like formulation of standards to be undertaken rapidly, in light of the fact that important authentication information (e.g., depositors' Internet banking login IDs and passwords) is currently being used in web scraping, in order to enable a smooth transition to APIs.

- Consideration of electronic message specification standards should revolve around the following details: 1) common items described in response messages (granularity of items included), 2) definition of common items, and 3) parameter description rules (or the pattern for such rules if multiple rules are permitted).

- When formulating electronic message specification standards, care should be taken to follow the development principles in Section 2.2, to allow for them to be expanded by individual banks, and to ensure that their positioning and scope do not impede the development of cutting-edge API-related initiatives by those involved.

- The electronic message specification standards should be published so that they may be referenced and freely used by a wide range of related-parties.

- As development of these standards moves forward, the opinions of various related-parties such as banks, IT companies, and Fintech companies, etc., regarding other points will be considered.

2.5 Other

a During the discussions relating to this report, multiple Fintech company members of the Committee expressed various preferences regarding detailed specifications for APIs to be developed by banks. Since many of these may be useful as references for individual banks when considering API specifications, they are described below.[34]

b When making revisions to the guidelines and so forth in future, the Committee will continue to bear these expectations and preferences in mind as needed.

[33] Excluding transfers between accounts at the same bank.
[34] Please note that items which are reflected elsewhere in the various guidelines have been omitted.

Expectations of Fintech Companies with Regard to Detailed API Specifications (Reference Examples)[35]

Connection specifications

- ✓ From the perspective of financial inclusion and increasing the financial services business, it is important not to restrict APIs to Internet banking activities and instead seek to meet a wide range of consumer needs by allowing APIs to be used even by customers without online banking contracts. It is therefore preferable to design APIs that are not predicated on the use of Internet banking.[36]
- ✓ At present, many APIs offered in Japan are delivered via Internet banking. In many cases, Internet banking contract numbers and passwords are used as authentication information, but consideration should also be given to the use of other authentication methods when conducting non-face-to-face transactions.[37]
- ✓ There are two kinds of read-only APIs: fetch-type APIs (whereby the third party goes to acquire banking information), and push-type APIs (whereby bank APIs deliver information to the service provider). There is a strong desire for the introduction of not just fetch-type but also push-type APIs; for corporate transactions in particular, it is assumed that development of EDI and XML APIs will lead to increased operational efficiency for client companies.

Scope of authorization specifications

- ✓ It is preferable that authorization specifications be defined to a moderate extent. If they are too detailed, there are concerns that users will scroll past them without reading or that some users will feel uneasy about the amount of responsibility involved.

Electronic message specifications

- ✓ Since it is possible that information acquired by APIs will not be in real time, due to batch or offline activities, it is preferable to implement attribute information that indicates it is current as of a certain date. In order to reduce processing loads for API provider-side systems, it may be made mandatory to stipulate a search range with specific dates and times when acquiring detailed information (i.e., specification that only provides new or modified details).
- ✓ Since Japanese bank account numbers have seven digits, if a field such as "account number" were specified, it would be designed with specifications for seven digits, which would be very helpful for third parties (for numbers with less than seven digits, 0s can be added at the start).
- ✓ Including account information verification functions with APIs could be beneficial to both API providers and customers, such as reducing the number of unprocessed transactions and avoiding the need for funds to be returned in the event of an erroneous deposit.
- ✓ Enabling customers to verify the results of transfers could eliminate or reduce the need for referring to API providers.
- ✓ By standardizing status codes for cases such as denial of access, it may be possible to determine the nature of errors based on the code alone.

Other

- ✓ If APIs are generally made widely available, it will be easy to publicize stub/mock environments, which would be helpful from an innovation perspective.
- ✓ Even after production migration, it is desirable that ongoing access to test environments be allowed (e.g., by setting aside specific time periods). It is necessary for Fintech companies to

[35] Information current as of March 2017.

[36] This report allows for the possibility of specifications that are not predicated on Internet banking—see, for example, "Authentication Relating to Granting Access Privileges" in Chapter 3 ("Security Measures and User Protection").

[37] See note 35.

conduct tests when upgrading versions themselves. (Third parties may also upgrade versions independently via APIs, assuming that this will have no impact.)

- ✓ In each environment, it is preferable that enough data required to cover test cases should be provided.

3. Security Measures and User Protection

3.1 Basic Approach

a The use of open APIs in the financial sector is currently in the trial phase in various countries around the world, and there are many points that need to be discussed. Security measures and user protection are particularly important issues with regard to ensuring confidence in services for users of open APIs, spreading and promoting open APIs.

b While open APIs are implemented based on requests and approvals from users, highly confidential customer information possessed by banks is provided to and gathered/saved by other companies such as Fintech companies ("third parties"), and banks also receive settlement instructions via third parties rather than users. Thus, when engaging in open APIs, it is necessary for the parties involved to ensure adequate security measures and user protection.

c On the other hand, if third parties are needlessly required to implement security and user protection measures that are equivalent to those of banks, there is a risk that it could impede the provision of highly convenient, innovative services through collaboration between banks and third parties, the enhancement of financial services, and initiatives aimed at innovation, meaning that users will miss out on opportunities to benefit from technological developments.

d Based on these considerations, the Committee has established a basic approach to security measures and user protection for open APIs in the banking sector (banking APIs) that aims to balance user convenience and user protection via a risk-based approach suited to the type of API functions,[38] related data, confidentiality issues and such.

e In establishing this approach, the Committee has made a conscious effort not to impede innovation, and by preparing guidelines for suitable standards for both banks and third parties. It was intended to eliminate issues such as banks demanding excessively conservative security measures from third parties or banks hesitating to engage in open APIs due to concerns over security, as well as to help facilitate smooth collaboration and partnership between banks and Fintech companies, etc.

f As mentioned earlier, open APIs are a key technology for enabling open innovation, and it is expected that this technology will be used to provide a wide range of business models and services. It is thus difficult to comprehensively consider all of the risks and countermeasures involved, which will vary depending on the business model and service. This report therefore focuses on security and user protection measures for major risks that are likely to be shared by various business models and services.

g With regard to specific security and user protection measures, there are many factors that need to be decided separately, depending on each bank's policies, individual businesses, the risks associated with different services, and the aspects of third parties. It is expected that those involved will give sufficient consideration to these matters

[38] For example, in the case of read/write APIs, if no settlement instruction maximum amount has been stipulated, it is possible that users could suffer significant damages due to unauthorized transfers.

from a user protection perspective while drawing on the points in this report. For example, in light of the details of a given risk, additional countermeasures that are not mentioned in this report may also be implemented. Conversely, reduced security measures may be considered for businesses and services which involve little risk.

h Security principles and user protection principles adapted to the main risks anticipated with open APIs are presented below.[39]

3.2 Major Risks of Open APIs

Open APIs will be used to provide users (depositors) with new services by setting up new communication pathways through other companies on systems of financial institutions. There is therefore a risk of these communication pathways being misused, leading to the leakage or falsification of data and unauthorized transactions. The major anticipated risks associated with open APIs are listed below.

3.2.1 Security-Related Threats and Risks

a Risk of leak of login IDs and passwords of third parties for some reason and used to access the third party without authorization

b Risk of third party systems being attacked, resulting in termination of service functions, large-scale leakage of data, falsification or loss of data and unauthorized money transfers.

c Risk of bank API-related systems that manage the issuing of tokens[40] being accessed without authorization and tokens being acquired without permission

d Risk of large-scale data leaks from banks due to leakage or counterfeiting of tokens, resulting in falsification or loss of information and unauthorized money transfers.

e Risk of information leaks, falsification or loss of information and unauthorized money transfers, due to hacking of communication pathways such as routers and interception of wireless communications.

f Risk of banking systems failure due to inadequacies in third party programs.

g Risk of unnecessarily large volumes of data being sent via bank open API communication pathways, thereby increasing the load on banking systems and impacting other banking services

---

[39] The meaning of various phrases used when describing the security principles and user protection principles is as follows:
- "must" signifies a measure that is strongly desirable in terms of societal norms.
- "necessary" signifies a measure that is expected to be a best practice for banks and third parties when using open APIs.
- "must strive to" signifies a measure that those involved are expected to work toward achieving.
- "may consider" signifies a measure that banks and third party may select at their own discretion.
- "is expected that" signifies an expectation that the Committee has of relevant institutions and organizations.

[40] A token is a permit holding authentication information for the purpose of linking applications of banks and other companies in OAuth 2.0 (the same applies below).

h Risk of internal executives and employees making unauthorized use of user information (including reselling and personal use)

i Risk of internal executives and employees using tokens without authorization in order to acquire account balance information or send unauthorized settlement instructions

3.2.2 User Protection-Related Risks

a Risk of doubts about third party activities or social credibility leading to users suffering damages or disruption due to the use of API-based services

b Risk of doubts about third party user protection status, financial credibility and means, resulting in users being unable to receive sufficient protection

c Risk of third parties not having a means of contacting users in the event of an emergency and being unable to take sufficient measures to protect customers

d Risk of users making use of API-based services without having a sufficient understanding of authority, risks and the purpose for which information acquired by API-based service providers will be used.

e Risk of users not knowing who to contact in the event of a problem

f Risk of users carrying out procedures without reading the relevant information carefully, even if efforts are made to properly explain and display it

g Risk of information provided by banks not being displayed properly because of problems and bugs in third party systems

h Risk of transactions between users/third parties and banks failing due to impediments caused by communication pathways between third parties and banks

3.3 Security Principles

3.3.1 Eligibility of Third Parties

Preliminary assessment

a Before banks allow other companies to access APIs, it is necessary to review the eligibility of third parties from a security perspective.[41] In the case of a bank connecting with a third party via a shared system, the shared system provider will provide access based on the results of the bank's review of the third party.

b When reviewing security-related eligibility, it is necessary for banks to verify the following items with third parties at the very least:[42]

- Fulfillment of security principles
- Past cases of improper security-related conduct and improvements made

[41] See Section 3.4.1 ("Eligibility of Third Parties") in Section 3.4 ("User Protection Principles") with regard to non-information security-related eligibility.

[42] If a third party uses ASP or cloud services, bear in mind that the service provider needs to disclose the required information.

- Whether or not the third party has arrangements in place and devotes resources to continuous enhancement of security measures based on user characteristics and transaction risks.

c Eligibility reviews should not be conducted in an inflexible or rigid manner, and it is necessary for banks to review other matters that they deem important, based on thorough API connection with companies, the specific risks associated and the individual bank's security policies.

d Banks may consider referring to security policies and security-related documents developed independently by third parties and information security-related certifications (e.g., ISO27001, TRUSTe) they have obtained when conducting the above eligibility review.

e In order to reduce the screening-related workload for banks and third parties, banks may use an information security-related organization to conduct reviews of third party eligibility. For this purpose, it is expected that information security-related organizations will establish an "API Connection Checklist" (provisional name) comprising required verification items and other independently determined verification items.[43]

f While it is assumed that banks will perform preliminary reviews independently, in order to reduce the screening-related workload for banks and third parties and standardize the criteria for preliminary reviews by banks, individual banks may consider entrusting preliminary reviews to other banks or referring to the results of preliminary reviews already conducted by other banks at the risk of the bank.[44]

Monitoring

g Even after API access is provided, it is necessary for banks to verify the information security-related eligibility of third parties, either on a periodic or an as-needed basis.[45]

h Banks may consider determining the monitoring method, extent and frequency on an individual basis, based on user characteristics, transaction risks, the intended business model of thorough API connection with companies that wish to access via APIs, the specific risks associated and the bank's security policies.

i With regard to API access, it is necessary for banks to agree upon monitoring-related items (e.g., method, extent, frequency, on-site inspections when required, actions to take if major changes are made to information security measures) with third parties in advance.

j If banks have concerns about the information security-related eligibility of third parties,

---

[43] The required verification items should be limited to as common detail as possible, so as not to place an excessive burden on third parties, and it is necessary to include information that makes it possible to conduct verifications focused on practical details relating to operations rather than pro forma details such as the number of people and amount of capital.

[44] If using this method, banks may consider referring to the joint audit method framework stipulated in FISC's Information System Audit Guidelines for Banking and Related Financial Institutions with regard to key points to bear in mind when making agreements with other banks.

[45] If a third party undergoes periodic information security-related monitoring by an external party, banks may consider using the results of these audits.

they must request that the third party make improvements and, if necessary in order to ensure user protection, limit, suspend, or terminate the access privileges of the third party.[46]

k While it is assumed that banks will perform monitoring independently, in order to reduce the monitoring-related workload for banks and third parties and standardize the criteria for monitoring by banks, individual banks may, on their own responsibility, consider entrusting monitoring to other banks or referring to the results of monitoring already conducted by other banks.[47]

3.3.2 Countermeasures for External Unauthorized Access

a The following items assume the use of a system implementing OAuth 2.0[48] for access privilege authorization. The items do not preclude use of other authorization/authentication protocols that enable equivalent or superior robustness (including new technologies).[49]

Authentication Relating to Granting Access Privileges

b Except when providing public information or anonymized information, banks must grant access privileges ("permission" in OAuth 2.0) to third parties based on user requests, and when doing so, they must verify user identity.

c It is necessary for authentication methods to be sufficiently robust based on user characteristics, the details of granted access privileges, and the associated risks.[50] For example, banks may consider that cases that involve the granting of settlement instruction rights require a more robust authentication method than cases that involve granting the right to obtain account balance and account activity.

d When selecting an authentication method, one goal is to meet the authentication method standards of other open network-based transaction channels being used by the bank (e.g., Internet banking), but it is necessary for banks to bear the following points in mind as well:

- It is authentication for access privileges permission, not authentication for individual transactions
- The authentication method relating to individual transactions that receive instructions via an API also needs to have sufficient authentication strength to handle all potential unauthorized access risks

e If an authentication method whose robustness is inferior to that of authentication

---

[46] However, care should be taken to ensure that arbitrary decisions by banks to limit access do not negatively affect the third party's business.

[47] If using this system, banks may consider referring to the joint audit method framework stipulated in FISC's Information System Audit Guidelines for Banking and Related Financial Institutions with regard to key points to bear in mind when making agreements with other banks.

[48] Standard relating to system flow for authorizing access privileges. It is generally available and may be referenced by any API developers. It is managed and administered by the IETF (Internet Engineering Task Force), an organization that develops standards for technologies used on the Internet.

[49] See Chapter 2 with regard to standardization of API specifications.

[50] Likewise, based on their own judgment, banks may consider using a more robust authentication method to ensure user protection.

methods for other open network-based transaction channels being used by the bank (e.g., if password authentication is accepted for users without an Internet banking contract), separate user protection-related measures will be necessary, given that the risk of unauthorized access will increase. For example, banks may consider the following measures: use in combination with over-the-counter procedures, confirmation by physical mail, setting a small amount as the upper limit for fund transfers, setting short validity periods for tokens, and stipulating in advance the compensation to be paid in the event that unauthorized usage occurs.

f For other points to bear in mind, banks may consider referring to documents such as: Comprehensive Guidelines for Supervision of Major Banks and Comprehensive Guidelines for Supervision of Regional Institutions, etc. (Chapter III-3-8/II-3-5: Internet Banking), the Inspection Manual for Deposit-Taking Institutions (Attachment 2-III-I-(5): Management of Transactions Conducted over Internet), the FISC's Security Guidelines on Computer Systems for Banking and Related Financial Institutions, and JBA's Matters to Be Considered in Internet Banking.

Management of access privileges/tokens

g It is necessary for banks to bear in mind the following points with regard to management of access privileges granted to third parties (issuing of tokens in OAuth 2.0):

- The granted access privileges should be limited to the scope required for the services to be provided by the third party (even if there is a request or consent from a user, unnecessary access privileges should not be granted to third parties)
- An appropriate validity period should be set for tokens issued to third parties, based on factors such as user characteristics, the nature of the access privileges and associated risks, and user convenience
- Measures should be taken to prevent the counterfeiting or fraudulent use of tokens, based on the nature of the access privileges
- If unauthorized access is detected or occurs, the bank should have a system that enables access privileges to be promptly limited, suspended, or terminated

h Banks must implement strong security measures for systems that manage access privileges and tokens. In addition, they must require third parties to implement appropriate token management and security measures.

Authentication relating to individual transactions

i Individual transaction instructions from users (e.g., instructions to acquire account balance or account activity, settlement instructions) are handled via a two-step authentication process: authentication handled by a third party when the user accesses that third party's system,[51] and authentication handled by a bank when it receives the individual transaction instruction from the third party.

[51] However, in cases where third parties provide settlement services via physical media using NFC (near-field communication) technology, individual transaction-related authentication by third parties is handled based on possession/usage of the physical media.

j In order to ensure user protection and prevent unauthorized access or information leakage, banks may consider, as a general principle, that the level of robustness for both of the authentications mentioned above should be equivalent or superior to the authentication methods for individual transaction-related instructions used for other open network-based transaction channels at the bank where the user has an account.

k If, for example, the bank where a corporate user has an account uses an authentication method for verifying account balance and account activity via Internet banking that does not depend solely on a fixed login ID and password (such as a variable password or electronic certificate), both the third party and the bank should, as a general principle, use an authentication method with equivalent or superior robustness.[52]

l On the other hand, robust authentication methods may involve a significant procedural burden to users or require significant investment by third parties in order to meet the requirements, so if these principles are applied in an inflexible manner, there is a risk that user convenience will decrease considerably or that it will not be possible to ensure the feasibility of user-friendly services.

m Therefore, banks may also consider ensuring user convenience while implementing thorough user protection suited to individual and corporate user characteristics and the risks associated with the transactions to be authenticated by combining the authentication method with other user protection measures and measures to prevent unauthorized access or information leakage. Examples of other user protection measures and measures to prevent unauthorized access or information leakage that may be combined with the authentication method include the following:

- In addition to token authentication, combining the bank's authentication method relating to fund transfer instructions with out-of-band authentication, and implementing direct authorization of users by the bank where required
- Using an authentication method that ensures user convenience while maintaining a certain level of authentication strength, such as biometric authentication, device authentication, or multi-channel authentication
- Either the bank or third party sends the user an email notification if funds are transferred
- Limiting the devices that users may use to access services to specific devices or specific types of devices that ensure security
- Using a closed network for communication between users and third parties, or communication between third parties and banks, or both types of communication
- Setting a short validity period for tokens (e.g., one-time only, expiring after a period of one to several months)
- Limiting the scope and period of provided information
- Limiting the funds transfer maximum to a small amount (e.g., setting the maximum funds per transfer as X yen and setting the maximum cumulative amount of funds that may be transferred based on a simple authentication method as Y yen)
- Only allowing funds to be transferred to accounts that are registered based on a

[52] Conversely, if, for example, a third party's authentication strength is inferior to the authentication strength for Internet banking, there will be higher risk of information leakage or the like occurring due to targeting of the vulnerable third party.

robust authentication process

- Only allowing funds to be transferred to other accounts at the same bank belonging to the same person
- Limiting services to users who possess certain characteristics (e.g., limiting services to individuals who meet certain characteristic requirements, limiting services to corporations, limiting services to affiliated companies or employees)
- The bank or the third party pays compensation to users in the event that unauthorized transfers or information leaks occur[53]
- Providing services that offer increased convenience but decreased authentication strength after obtaining a full understanding and consent of users regarding the risks involved
- Receiving settlement instructions directly from users rather than via third parties[54]

n Combining the authentication method with items such as the examples above does not mean the authentication strength can immediately be reduced; even after the authentication method that is used has been combined with other user protection measures like those above, it is necessary to fully ensure that user protection is suited to the characteristics of individual or corporate users, and the risks associated with the transactions to be authenticated.

Communication method

o If using an open network for the communication method, it is necessary to protect it using TLS in order to prevent theft.

System robustness

p Banks have an obligation to maintain the confidentiality of customer information in accordance with standard business practices and private law based on the principle of good faith. In addition, based on the Banking Act (Article 13-3-2, "Establishment of a System for Protecting the Customers' Interests" and such), Guidelines for Personal Information Protection in the Financial Field, Comprehensive Guidelines for Supervision of Major Banks and Comprehensive Guidelines for Supervision of Regional Institutions, etc. (Chapter III-3-3-3/II-3-2-3: Arrange Managing of Customer-Related Information, Chapter III-3-7/II-3-4: System Risks), the Inspection Manual for Deposit-Taking Institutions (Attachment 2), FISC's Security Guidelines on Computer Systems for Banking and Related Financial Institutions, the All Banks Personal Data Protection Council's Personal Information Protection Guidelines and Guidelines Relating to Measures for Secure Management of Personal Data, and others, banks are required to properly manage information relating to their activities, establish a system to appropriately monitor the implementation of their activities, and take any other necessary measures to ensure that undue harm is not caused to customer interests. Furthermore, under the terms of the Banking Act, if their arrangements in this regard are inadequate, they may be ordered to make improvements to their business.

[53] However, it is necessary to give consideration to the fact that even if compensation is provided for damages, there is a risk that large sums of money could be stolen by anti-social elements if no fund transfer maximum is stipulated.

[54] As of June 2017, the W3C (World Wide Web Consortium), a non-profit organization that promotes the standardization of various technologies used online, is considering a system (payment request APIs) that uses user browsers to send settlement instructions directly to banks.

q In light of the confidential nature of customer information possessed by banks, third parties (especially PFM businesses that collect large amounts of information about customers from multiple banks) should ideally implement security measures that are equivalent to those of banks in order to ensure user protection and prevent unauthorized access or information leaks; however, it is not necessarily appropriate to rigidly apply all the above banking business-related security management measures to third parties. Furthermore, while the approach to system risk management for outsourcing contractors of banks stipulated in the Banking Act, Guidelines for Supervision and Inspection Manual may serve as a reference, using open APIs is different from outsourcing to external contractors. Provision of information from banks to third parties is based on requests/consent from users, and part of a bank's system, which requires a high level of robustness, is not outsourced to a contractor; it may therefore not be possible to rigidly apply the framework for managing external contractors to open APIs.

r With regard to the standards for safety management measures that should be met by third parties, it is fundamentally necessary for third parties to judge these for themselves based on the risks involved, taking into account factors such as the type and quantity of information that they will obtain and store, the presumed impact and damages to users in the event that information is leaked, and user expectations of third parties in terms of information management.

s It is expected that information security-related organizations will develop basic approaches and points to bear in mind with regard to standard safety management targets that should be met by third parties. However, as a bare minimum, it is necessary for third parties to implement the following measures:

- Installation of anti-virus software
- Encryption of highly confidential information (e.g., third party login passwords, client certificates, tokens)
- Installation of multi-layered defenses against cyberattacks, such as firewalls
- Server modification monitoring (to detect tampering) and network monitoring
- Public server vulnerability countermeasures
- Acquiring and saving API activity logs (users, operations, results)
- Countermeasures in case of loss of information (e.g., backing up)

t The way to handle personal information (individual data) that banks provide to third parties with customer consent should be determined on a case-by-case basis depending on the specific arrangement, in accordance with the Act on the Protection of Personal Information, but as a general rule, banks may reasonably interpret the law as meaning that the obligation to supervise businesses entrusted with personal information (see Article 22 of the Act) does not apply in the case of third parties.

<u>Unauthorized activity detection/monitoring functions</u>

u Unauthorized activity detection/monitoring functions are essential in order to actively prevent damages occurring or increasing in scope due to unauthorized access.

v FISC's Security Guidelines on Computer Systems for Banking and Related Financial

Institutions provide a framework for banks to detect and monitor data falsification, unauthorized access, and unauthorized or irregular transactions.

w In the case of open APIs, banks are unable to directly obtain information used to detect unauthorized activity, such as the user's IP address or the number of authentication failures. Therefore, if banks deem it necessary based on the transaction risks, it will be necessary to establish a system for third parties to supply banks with the information required to detect unauthorized activity.

x It is expected that information security-related organizations will develop a basic approach and points to bear in mind when deciding whether third parties also require unauthorized activity detection and monitoring functions and the standards that need to be met, taking into account factors such as the type and quantity of information that they will obtain and store, the presumed impact and damages to users in the event that information is leaked, and user expectations of third parties in terms of information management.

3.3.3 Countermeasures for Internal Unauthorized Access

a Countermeasures for external unauthorized access may not have any effect on internal unauthorized access. Thus, it is necessary for both banks and third parties to also implement countermeasures for internal unauthorized access.

Countermeasures for internal unauthorized access at banks

b The Banking Act (Article 13-3-2, "Establishment of a System for Protecting the Customers' Interests"), Guidelines for Personal Information Protection in the Financial Field, Comprehensive Guidelines for Supervision of Major Banks and Comprehensive Guidelines for Supervision of Regional Institutions, etc. (Chapter III-3-3-3/II-3-2-3: Arrangements for Managing Customer-Related Information, Chapter III-3-7/II-3-4: System Risks), the Inspection Manual for Deposit-Taking Institutions (Attachment 2), FISC's Security Guidelines on Computer Systems for Banking and Related Financial Institutions, and others provide a framework for banks to prevent unauthorized internal access. Furthermore, under the terms of the Banking Act, if their arrangements in this regard are inadequate, they may be ordered to make improvements to their business.

Countermeasures for internal unauthorized access within third parties

c In light of the confidential nature of customer information possessed by banks, third parties (especially PFM businesses that collect large amounts of information about customers from multiple banks) should ideally implement security measures that are equivalent to those of banks in order to ensure user protection and prevent unauthorized access or information leaks (including personal viewing, use, or resale by executives and employees); however, it is not necessarily appropriate to rigidly apply all the above banking business-related security management measures to third parties. Furthermore, while the approach to system risk management for outsourcing contractors of banks stipulated in the Banking Act, Guidelines for Supervision and Inspection Manual may serve as a reference, open APIs do not involve part of a bank's system being outsourced to a contractor, so it may not be possible to rigidly apply the framework for managing external contractors.

d With regard to the standards for internal unauthorized access countermeasures that should be met by third parties, it is fundamentally necessary for third parties to judge these for themselves based on the risks involved, taking into account factors such as the type and quantity of information that they will obtain and store, the presumed impact and damages to users in the event that information is leaked, and user expectations of third parties in terms of information management.

e It is expected that information security-related organizations will develop basic approaches and points to bear in mind with regard to standard internal unauthorized access countermeasure targets that should be met by third parties. However, as a bare minimum, it is necessary for third parties to implement the following measures:

- Specifying and managing appropriate system access privileges for executives and employees
- Saving, storing, and periodically reviewing access logs
- Providing education and training for executives and employees
- Server room monitoring, authentication, and access management[55]
- Restricting or prohibiting copying data such as important confidential information or customer information to USB drives or other media
- Managing the removal, deletion, or disposal of data including important confidential information or customer information

3.3.4 Handling Unauthorized Access

System design/specifications

a In the event that banks or third parties detect unauthorized access, the system design and specifications must enable the bank to promptly restrict, suspend, or terminate access privileges and the third party to promptly restrict or suspend service usage, in order to actively prevent damages occurring or increasing in scope.

b In order to handle inquiries from users regarding suspicious fund transfers, identify the cause when unauthorized access occurs, and consider any required countermeasures. Banks and third parties must save and store access logs in an appropriate manner.

Information sharing and discussion of countermeasures

c In the event that unauthorized access is detected, it is necessary for banks and third parties to promptly share information and collaborate on identifying the cause and discuss required countermeasures.[56] It is necessary for banks and third parties to decide on and clarify any required measures together before implementing them.

3.3.5 Continuous Improvement, Review, and Enhancement of Security Measures

a While the techniques employed in cyberattacks and other cybercrimes are becoming

[55] If using cloud-based services, this should be based on "Using Cloud-Based Services" in FISC's Security Guidelines on Computer Systems for Banking and Related Financial Institutions.

[56] With regard to other measures in the event that unauthorized access occurs, refer to Section 3.4.4 ("Actively Preventing Incidence and Spread of Damages") in "3.4 User Protection Principles."

more and more sophisticated each year, provision of open API-based financial services is currently in the initial stages around the world. As a result, it is necessary for banks and third parties to pursue continuous improvement, review, and enhancement of security measures, taking into account incidents of unauthorized access not just internally but at other companies as well.

b It is essential for banks and third parties to work together in pursuit of improvement, review, and enhancement of security measures.

3.4 User Protection Principles

3.4.1 Eligibility of Third Parties

Preliminary review

a Before banks allow other companies to access APIs, it is necessary for them to review the eligibility of third parties from a user protection perspective.[57] In cases where a bank connects with a third party via a shared system, the shared system provider will provide access based on the results of the bank's review of the third party.

b When reviewing eligibility, it is necessary for banks to verify the following items with respect to third parties at the very least:

- Details of business activities (including group companies) and subsidiary business activities
- Social credibility (including whether the company has relationships with anti-social elements) and organizational governance
- Legal compliance status
- User protection measures[58]
- Fulfillment of user protection principles
- Past cases of improper user protection-related conduct and improvements
- Whether or not the third party has arrangements in place and devotes resources to continuous enhancement of user protection measures based on user characteristics and transaction risks

c Eligibility reviews should not be conducted in an inflexible or rigid manner, and in addition to the items above, it is necessary for banks to review other matters that they deem important, based on the intended business model of companies that wish to access APIs, the specific risks associated with it and the individual bank's customer protection management regulations.

d In addition, banks may consider referring to internal regulations developed by third parties when conducting the above eligibility review.

e In order to reduce the screening-related workload for banks and third parties, banks

[57] With regard to information security-related eligibility, refer to Section 3.3.1 ("Eligibility of Third Parties") in "3.3 Security Principles."

[58] In particular, banks should verify whether the third party has made appropriate arrangements for handling and managing customer information, the appropriateness of the purposes for which acquired information will be used, and the appropriateness of the usage agreements (presence of terms that are notably insufficient from a user protection perspective, such as excessive exemption clauses).

may use an information security-related organization to conduct reviews of third party eligibility. For this purpose, it is expected that they will establish an "API Connection Checklist" (provisional name) comprising required verification items and other independently determined verification items.[59]

f While it is assumed that banks will perform preliminary reviews independently, in order to reduce the screening-related workload for banks and third parties, and standardize the criteria for preliminary reviews by banks, individual banks may consider entrusting preliminary reviews to other banks or referring to the results of preliminary reviews already conducted by other banks.[60]

Monitoring

g Even after API access is granted, it is necessary for banks to verify the eligibility of third parties, either on a periodic or an as-needed basis.

h Banks may consider determining the monitoring method, extent and frequency on an individual basis, based on user characteristics, transaction risks, the intended business model of companies that wish to access APIs and the specific risks associated, the bank's customer protection management regulations and such.

i With regard to API access, it is necessary for banks to agree upon monitoring-related items (e.g., method, extent, frequency, information that third parties will be required to provide, actions to take if third parties significantly revise their arrangements or stop doing business) with third parties in advance.

j If banks have concerns about the user protection arrangements-related eligibility of a third party, they must request that the third party make improvements and, if necessary in order to ensure user protection, limit, suspend, or terminate the third party's access privileges.[61]

k While it is assumed that banks will perform monitoring independently, in order to reduce the monitoring-related workload for banks and third parties and standardize the criteria for monitoring by banks, individual banks may consider, on their own responsibilities, entrusting monitoring to other banks or referring to the results of monitoring already conducted by other banks.[62]

Other important considerations

l If third parties involved in incidents where they were deficient in terms of ensuring

---

[59] The required verification items should be limited to extremely common details, so as not to place an excessive burden on third parties, and banks may consider it necessary to include information that makes it possible to conduct verifications focused on practical details relating to operations rather than pro forma details such as the number of people and amount of capital.

[60] If using this system, banks may consider referring to the joint audit method framework stipulated in FISC's Information System Audit Guidelines for Banking and Related Financial Institutions with regard to key points to bear in mind when making agreements with other banks.

[61] However, care should be taken to ensure that arbitrary decisions by banks to limit access do not negatively affect the third party's business.

[62] If using this system, banks may consider referring to the joint audit method framework stipulated in FISC's Information System Audit Guidelines for Banking and Related Financial Institutions with regard to key points to bear in mind when making agreements with other banks.

user protection for financial services provided via an API, it is necessary for banks to bear in mind that there is a risk that this could harm their reputation by exposing them to public criticism, depending on their relationship with the third party.

m If a service provided by a third party is effectively a substitute for a service provided by a bank (e.g., Internet banking) and the bank stops providing that service and recommends that depositors use the third party's service instead, it is necessary to bear in mind that, even if there is no formal outsourcing agreement between the bank and the third party, the relationship may be treated in the same manner as an outsourcing arrangement and be subject to outsourcing regulations under the Banking Act.

n If a service provided by a third party is effectively a substitute for a service provided by a bank (e.g., Internet banking) and if the majority of users rely on using the third party's service, it is necessary to bear in mind the risk of users being unable to use the service or being disrupted due to third party-related reasons (e.g., system failure, cessation of business).

o It is necessary to agree in advance that in the event that there is a risk that problems on the third party's side will impact the bank's business, the third party will notify the bank immediately. It is also important to bear in mind the need to decide in advance on other matters such as whether a report is required when a problem occurs and the timing of said report.

p It is necessary to specify an advance notice with a certain period of time to be provided if either the third party or the bank decides to suspend a service due to circumstances.

3.4.2 Explaining/Displaying Information and Obtaining Consent

Displaying important information and obtaining consent

a Typically, when it comes to Internet-based transactions, users make decisions and give consent based on information displayed on screen, and there is a possibility that even if the required information is displayed, users will proceed without reviewing it carefully.

b Therefore, it is not enough for banks and third parties to simply provide/display the information required for users to make decisions and give consent. They must strive to employ a display method and screen configuration that prioritizes user protection by displaying information on-screen in a user-friendly way, avoiding presenting it in a manner that leads to misunderstandings or misperceptions, implementing a process for alerting users when an important decision or approval is requested, requesting consent based on system operation by users.

c When issuing tokens, it is necessary at the very least for banks to clearly display the following points on screen in a user-friendly way when requesting consent from users:

- The name of the third party to which access privilege is granted
- The name of the API-related service
- The details and scope of the rights to be granted
- The validity period of the rights to be granted[63]

[63] If issuing refresh tokens, this is the maximum validity period that is possible by renewing the same token.

- How to delete or terminate granted rights
- Any other matters about which users need to be aware

d When providing services, it is necessary at the very least for third parties to clearly display the following points on screen in a user-friendly way when requesting consent from users:

- The purposes for which personal information will be used and the extent to which it will be shared (e.g., whether or not it will be provided to third parties), in accordance with the Act on the Protection of Personal Information
- Matters relating to deletion of acquired information
- Restrictions on service usage
- Any other matters about which users need to be aware

Displaying information about risks and such

e Third parties must strive to display the main risks associated with the services they provide in an appropriate manner.

f Third parties must strive to display the time periods when services are available and not available and restrictions on service provisions during closing hours and off days.

Preventing misunderstanding by users

g Banks must bear in mind the following points that are especially likely to be misunderstood or misperceived by users and strive to display information about them in an appropriate manner:

- The fact that services provided by a third party differ from services provided by the bank
- The relationship and respective roles of the bank and the third party (especially the fact that the third party is neither an agent nor an outsourcing contractor of the bank)
- Distinguishing between settlement instruction transactions and other services
- Distinguishing between the bank's screens and third party screens

h If a bank discovers that a third party has displayed false or intentionally misleading information, it must demand that the third party correct it and, if necessary in order to ensure user protection, take steps such as restricting, suspending, or terminating the third party's access privileges or notifying the relevant authorities.

Other displayed information

i It is necessary for banks and third parties to agree in advance on their respective responsibilities and the workflow in the event of user requests, consultations, complaints, or inquiries.

j It is necessary for banks and third parties to display contact information for handling user requests, consultations, complaints, and inquiries, based on the details of the above agreement.

k It is necessary for third parties to display information such as their trade name, company representative, address, and contact information.

l If third parties choose to disclose their financial results by electronic means, it is also necessary for them to display information about the announcement of their financial results in accordance with the Companies Act.

3.4.3 Actively Preventing Unauthorized Access

a In order to actively prevent unauthorized access, third parties must strive to alert users regarding the following points, among others:

- Users should set a password for logging in to third party services that differs from the password they use for banking services
- Users should avoid setting login passwords for third party services that are easy to infer and manage their password with care (e.g., not provide or disclose it to third parties, change their password periodically)
- Users should install anti-virus software

b It is necessary for third parties to ask users to contact them immediately if their password is lost or leaked or they suspect unauthorized access has occurred.

3.4.4 Actively Preventing Incidents and Spread of Damages

Initial response

a In the event that a bank or a third party detects unauthorized access, it is necessary for the bank to promptly restrict, suspend, or terminate access privileges and the third party to promptly restrict or suspend service usage, in order to actively prevent damages from occurring or increasing in scope.

b In order for both banks and third parties to promptly restrict or suspend functions and take any other required steps, if one party detects that API-related unauthorized access or information leakage/disclosure has occurred, it is necessary for it to immediately notify the other party. For this purpose, the parties should make any arrangements that are required to prevent damages from increasing in scope in advance, such as agreeing on the contact number and contact method to be used to communicate with each other in such a case.

c In cases where a third party is connected to multiple banks, if there is a risk of a similar incident occurring at other banks, the third party must strive to immediately notify the other banks involved and actively prevent the damages from increasing in scope.

Contacting users

d It is necessary for third parties to ensure in advance that they have a communication method for contacting users, so that they may notify any users who have been affected by a problem or promptly provide proper alerts to users who could potentially be affected (e.g., a notice asking them to change their password immediately).

e The scope of the communication method used to request users that they complete a registration process may be determined separately in accordance with the details of the provided service and associated transaction risks.

f If a third party is unable to ensure in advance that it has an adequate communication method for contacting users, in the event of a problem, it is necessary for banks to bear in mind that they may need to contact users and alert them instead of the third party.

3.4.5 Responsibilities and Compensation for Users[64]

a With open APIs, both third parties and banks are involved in processing and executing transaction instructions, so in the event that users suffer damages due to information leakage, unauthorized fund transfers, system-related problems and such, there is a risk that it may not be clear where the responsibility lies, who should be contacted, and who will address the issue.

b If the law is relied on to determine which party bears ultimate civil liability for damages, there is a risk that prompt recovery and compensation for damages will not be possible and that users will not be adequately protected.[65]

Prior agreement between the parties

c In order for banks and third parties to ensure prompt recovery and compensation for users, they must agree in advance on who should be contacted if unauthorized access, information leakage, unauthorized fund transfers, system-related problems or such occur, the means by which compensation or repayment will be made in the event of damages to users (including the party responsible),[66] and the extent of coverage.[67] Banks and third parties may not make agreements that are notably deficient in terms of ensuring user protection (e.g., agreements in which neither party bears any responsibility toward users).[68]

d Third parties and banks must publish the user compensation and repayment method and extent of coverage (including reasons for exemption of liability) agreed in advance between them so that users can access the information at all times (e.g., on their websites). In addition, they must strive to ensure that users are fully aware of who to

[64] The report of the Financial System Council's Working Group on the Financial System published on December 27, 2016, states that "in agreements made with other businesses, financial institutions [...] shall define and make public the division of responsibilities in the event of damages to customers" (see p. 8 of the report). Based on this statement, this section discusses rules relating to dividing up responsibilities for damages between banks, third parties, and customers while ensuring adequate user protection.

[65] This section discusses initiatives that third parties and banks are expected to undertake voluntarily in order to ensure user protection; these do not increase or decrease their ultimate legal responsibility to users.

[66] It is preferable that banks and third parties also make a separate advance agreement regarding their respective internal contributions (claims for compensation) once users have been compensated or repaid.

[67] Even if banks and third parties agree to assume collective responsibility toward users, there is a risk that who should be contacted, which party will address the matter, etc., will not be clear to users, so it is preferable that both sides agree in advance on a single initial compensation/repayment method (including which party will handle it) as they see fit.

[68] It is assumed that banks will need to carefully examine the third party's usage agreements to make sure that there are no provisions which limit its responsibility in an inappropriate manner, based on the Consumer Contract Act and other laws.

contact and how to contact them if they wish to request compensation or repayment; for example, third parties could display this information in an easy-to-understand method on the screen that appears when users finalize their contract.

Considerations regarding details and scope of compensation

e With regard to unauthorized debits from a deposit account made by means of API-based services, even in cases where the bank and third party have not been negligent, it is necessary for one of them to compensate individual users who suffer damage through no fault of their own, based on the prior agreement described above. In cases involving negligence or gross negligence on the part of the user, it is necessary to make a separate decision (including whether the user shall be held responsible for some or all of the amount), taking into consideration factors such as the situation/circumstances of the user who suffered the damages.

f Corporate users are likely to have relatively greater response capabilities for security measures than those for individual users. Given the possibility of unauthorized use due to the user's usage environment or security level, it is important to make efforts to prevent damages from unauthorized usage by implementing security measures on both the service provider side and the user side. In light of this, it is necessary to make decisions regarding compensation to corporate users on a case-by-case basis, taking into account factors such as the security measures implemented by the user, the circumstances with regard to prevention of damages from unauthorized usage, the corporation's characteristics, and the response capabilities of its security measures.

g In cases where banks and third parties have valid reasons for deciding that the details and scope of compensation should differ from the above, in light of factors such as the type of API-based service and user characteristics, they may stipulate different compensation details and scope, as long as they explain or display the relevant information to users in an appropriate manner in order to avoid the incidence of unforeseen damages to users.

Points to consider if third parties are responsible for compensation or repayment

h In cases where a bank and a third party reach an agreement that the latter will be responsible for compensating or repaying users, it is necessary for the bank to evaluate its fitness bearing in mind that there is no risk of the third party being unable to ensure user protection (e.g., it has made the necessary arrangements and has sufficient resources to compensate or repay users) and to review its situation on a periodic or an as-needed basis.

i If a bank judges that a third party may be unable to ensure user protection (e.g., it has not made the necessary arrangements or lacks sufficient resources to compensate or repay users), it is necessary for the bank to demand that the third party revise its arrangements, increase its non-exempt property, and acquire liability insurance and, if it is difficult for the third party to meet these requests, take measures such as withholding API access (or considering suspending or terminating access).

j If there is a concern that a third party's usage agreements provide excessive reasons for exemption from liability (e.g., no negligence liability[69]) or that it may not actually

[69] Clauses which fully exempt a business operator from liability to compensate consumers for damages

fulfill its responsibility to compensate or repay users, it is necessary to demand that it revise them, based on the Consumer Contract Act and other laws.

3.5 Other

Handling of public information

a If public information that can be obtained without the need for procedures such as logging on to a bank's website (e.g., addresses of branches and ATMs) is provided to a third party (hereafter referred to as "public information"), it can be handled as follows, irrespective of the preceding explanations:

- In order to prevent the falsification of information, the communication method used for communication pathways between the bank and third party should be based on the provisions regarding communication methods stipulated in Section 3.3.2 ("Countermeasures for External Unauthorized Access") of the security principles.
- If a situation arises in which there is a possibility that the bank will receive inquiries from users due to a problem with the third party's system, falsification resulting from an external, internal attack or such, the third party must strive to notify the relevant bank immediately.
- It is preferable that banks stipulate in advance their responsibilities in the event that problems occur in the API usage agreements
- If the bank is unable to control the amount of traffic for the API via which public information is provided, it should bear in mind the risk of problems occurring due to the system capacity being exceeded.

Handling third parties of the third party

b It is necessary for banks to agree with third parties in advance on how they will handle any third parties of the third party ("linked third parties"[70]).

c Various methods of handling linked third parties may be considered, including: handling in the same manner as third parties (i.e., the bank makes an agreement directly with the linked third party); making it a condition that the bank's approval be obtained or prior notice be provided with regard to linked API-based service provision; deciding in advance on the conditions for accepting linked service provision, based on discussion between the bank and third party; permitting linked service provision if the third party takes responsibility for and manages it.[71]

d Regardless of the method used, it is necessary for linked third parties to implement

---

arising from default by the operator, clauses which partially exempt business operators from liability to compensate consumers for damages arising from default by the operator due to an intentional act or gross negligence on the part of the operator, its representatives, or its employees, and similar clauses are inherently void under the terms of the Consumer Contract Act (Articles 8 to 10).

[70] In cases where transaction instructions from a third party to a bank are issued based on transaction instructions from another business with access to the API, this term refers to the other business.

[71] Handling of linked third parties may differ depending, for example, on the differences in the transaction risks associated with read-only APIs and read/write APIs and whether the linked third party belongs to the same group as the third party.

proper security measures and ensure user protection, based on the contents of the present guidelines.

e Provision of information about a third party to other businesses via the provider's own APIs does not constitute linked API service provision, but it is important to bear in mind the need to ensure appropriate user protection based on the Act on the Protection of Personal Information and other laws.

Applicability of Guidelines to non-banking APIs

f The Committee hopes that the security principles and user protection principles outlined in this report will serve as a reference for businesses in sectors other than banking engaged in open APIs when they are developing security measures and user protection arrangements.

4. Future Initiatives

4.1 Initiatives Relating to Standardization of API Specifications

a Under the administration by JBA, there are plans to proceed with standardization of electronic message specification for deposit-related transfers while taking into account the views of various related-parties, such as banks, IT companies and third parties.[72]

b In addition, if further standardization of specifications becomes necessary in future with the development of new API-based services, it is expected that similar consideration will be given to these.

4.2 Collaboration with Information Security-Related Institutions

Establishment of API Connection Checklist

a In order to reduce the screening-related workload for banks and other companies accessing APIs, it is expected that banks will establish an "API Connection Checklist" (provisional name) to use when reviewing the eligibility of third parties.[73]

b With this in mind, FISC established an API Connection Checklist (Provisional Name) Working Group in February 2017, which is currently considering the formulation of this checklist.

c The Committee welcomes FISC's efforts, which it expects will help facilitate future collaboration and partnership between third parties and banks and reduce communication costs relating to security measures and such, for both sides.

Initiatives aimed at sector/industry-wide enhancement of security measures

d The techniques employed in cyberattacks and other cybercrimes are becoming more and more sophisticated each year. Given that open APIs are a system for providing other businesses with access to bank systems, if there are vulnerabilities in the API system, there is a risk that this could lead to system trouble or, in the worst-case scenario, unauthorized fund transfers or leakage of customer information.

e Since open APIs are a new technology at the present time which is not yet mature in terms of usage and specifications, in addition to implementing measures at individual banks, it is important to collaborate with information security-related institutions on developing a framework for sector/industry-wide sharing of information about unauthorized access incidents and security-related measures and to support continuous improvement, review, and enhancement of security measures by banks and third parties.

f With this in mind, as an initiative aimed at raising the level of Fintech-related security measures across the sector as a whole, Financials ISAC Japan, which shares information, conducts analysis and such, with regard to cyber security,[74] has

[72] Electronic message specification standards for deposit-related balance and account activity inquiries have already been formulated in a separate document.
[73] Refer to Chapter 3 ("Security Measures and User Protection Principles").
[74] http://www.f-isac.jp/

established a Fintech Security Working Group that includes representatives of financial institutions and third parties, which is currently working on policies that focus on information collection and sharing in relation to open API security.

g The Committee welcomes Financials ISAC Japan's efforts, which it expects will support open API initiatives with a high level of security and convenience at Japanese financial institutions.

4.3 Initiatives Aimed at Facilitating Collaboration and Partnership Between Banks and Fintech Companies, etc.

a A report by the FISC Working Group on the Financial System ("Financial System WG") on system development aimed at open innovation published on December 27, 2016,[75] encourages collaboration and partnership between banks and Fintech companies, etc., and in order to promote open innovation, it states that financial institutions should formulate and publish their criteria for deciding on whether or not to enter into agreements with electronic payment intermediate third parties.

b On the other hand, since there are a great many banks in Japan,[76] comprehensively reviewing decision-making criteria published separately by each bank (e.g., on its website) and contacting individual banks will involve a heavy workload for Fintech companies, etc. Moreover, even if banks actively pursue collaboration and partnership with Fintech companies, etc., there is a risk that they could miss out on opportunities for innovative collaboration and partnership if the workload involved in verifying information is excessive.

c In order to facilitate collaboration and partnership between banks and Fintech companies, etc., JBA, based on the direction outlined by the Financial System WG and relevant laws and regulations, is expected to make efforts to collect and publish information about the current implementation status of open API-related initiatives (e.g., publication of decision-making criteria by each member bank, establishment of contact point for inquires by each member bank) in list format or the like, with the consent of the relevant banks.

d In addition, the Committee recognizes the importance of collaboration and communication between the banking sector and the Certified Electronic Payment Intermediate Service Provider Association that is set to be formed in future[77] when it is deciding on the specific nature of its activities. When the Association formulates regulations required for the purpose of secure management and measures to protect the interests of users in particular, the Committee hopes that the Association will draw on the security and user protection principles outlined in this report.

4.4 Revisions to This Report and Ongoing Communication

<u>Revisions based on related laws and regulations</u>

[75] http://www.fsa.go.jp/singi/singi_kinyu/tosin/20161227-1.html

[76] JBA has 120 full members, 71 associate members, and 1 sub-associate member.

[77] See Article 52-61-19, etc., of the revised Banking Act based on the Act for Partial Revision of the Banking Act (enacted on May 26, 2017) as well as the appendix to this report, "About Registered Businesses and the Certified Electronic Payment Intermediate Service Provider Association").

a The Committee's secretariat will consider the need to revise this report based on the development of relevant laws and regulations, and it is expected that it will work with Committee members to make any revisions that are required.

Ongoing collaboration and communication between the banking sector and the organization of third parties

b Since open API initiatives are still in the early stages around the world, it is important for the banking sector to pursue ongoing collaboration and communication with the industry organizations of third parties, IT companies and such, with regard to new challenges and issues that arise.

c With this in mind, it is expected that banks and organizations related to third parties will take steps such as establishing venues for exchanging opinions on an ongoing basis, following discussion between the relevant parties.

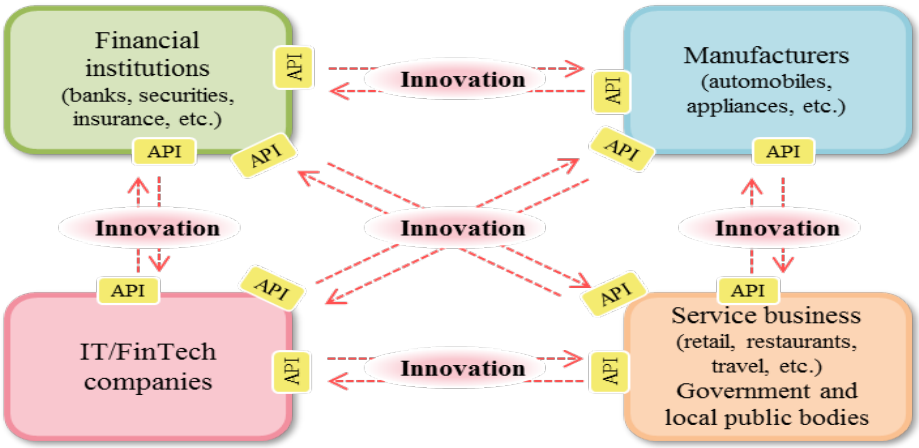
Other revisions

d The Committee's secretariat is expected to give consideration to reviewing and revising this report as needed in light of new developments and so forth.[78] The secretariat has created an email address, open-api@zenginkyo.or.jp, for those who wish to provide feedback on this report, which will be taken into consideration when deciding whether or not to make revisions.

[78] The method, framework and such, for making revisions to this report shall be considered by the secretariat on a case-by-case basis, according to the specific details.

4.5 Aiming for the Development of an API Ecosystem

a With the aim of stimulating open innovation, it is important that not just banks but also other businesses develop open API initiatives and that an API ecosystem enabling valuable information to be exchanged between businesses in various industries, not just the banking sector, is formed.



b The Committee expects that the pursuit of open API-based initiatives in the banking sector will trigger the development of open API initiatives by non-banking businesses as well, which will help to establish the aforementioned API ecosystem.

Addendum

About Registered Companies and the Certified Electronic Payment Intermediate Service Provider Association

a Article 52-61-19, etc., of the revised Banking Act based on the Act for Partial Revision of the Banking Act (enacted on May 26, 2017) establishes a framework for a Certified Electronic Payment Intermediate Service Provider Association in order to promote voluntary initiatives by an industry organization.

b Voluntary initiatives undertaken by an industry organization such as this have an important role to play in facilitating efficient open innovation involving electronic payment intermediate third parties and financial institutions while at the same time ensuring effective user protection. It will also be important for the Committee to respond to this development and collaborate and communicate with relevant parties in an appropriate manner.

c It is therefore necessary that the scope of the criteria for companies to register as certified electronic payment intermediate third parties, which will determine eligibility for membership in the Certified Payment Electronic Intermediate Service Provider Association, be fully publicized. For example, since regular account transfer services are considered separate from settlement instruction communication services, companies that provide the former services will not be eligible to register, whereas companies that provide cloud-based accounting services or, based on the provisions of the revised Act, provide non-regular services such as real-time account transfer services and account transfer services using Pay-easy, will likely be eligible to register. Going forward, it will be necessary for the relevant authorities to properly publicize and explain the details of the registration system to eligible companies, including those mentioned above.